каждому совершеннолетнему гражданину, что позволит избежать повторного голосования путем создания нескольких учетных записей, с целью повышения количества голосов за кандидата.

## АНАЛИЗ ДЕЙСТВУЮЩИХ ПОЛИТИК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОАО «РЖД» В СВЕТЕ ОСОБЕННОСТЕЙ СИСТЕМ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

*Е. О. Чигринский, Т. Ю. Зырянова*
(Екатеринбург, УрГУПС, echigrinskiy@gmail.com)

На опыте работы крупнейших мировых компаний можно убедиться, что игнорирование вопросов информационной безопасности весьма увеличивает риск возникновения серьезных материальных потерь вплоть до остановки технологического процесса. На данный момент количество попыток несанкционированных воздействий на корпоративные информационные ресурсы существенно возросло. Информационные системы ОАО «РЖД» представляют собой потенциальный источник информации, которая может быть использована в целях совершения различных противоправных акций. Именно поэтому стоит уделять пристальное внимание проблеме обеспечения информационной безопасности. И именно поэтому стратегия развития ОАО «РЖД» до 2030 г. включает в себя и задачи по обеспечению безопасности на объектах железнодорожного транспорта.

Приведем примерный перечень таких задач [1]:

- совершенствование основных положений государственной политики и нормативной правовой базы обеспечения безопасности объектов инфраструктуры железнодорожного транспорта и их реализация;
- разработка комплекса мероприятий по реализации положений государственной политики и приоритетных направлений обеспечения безопасности транспортной системы России в области железнодорожного транспорта;

• разработка методологии и практических методов решения задач обеспечения безопасности на объектах железнодорожного транспорта;

• определение состава угроз безопасности объектов железнодорожного транспорта;

• проведение категорирования и оценки уязвимости объектов железнодорожного транспорта;

• разработка системы требований по обеспечению безопасности объектов инфраструктуры железнодорожного транспорта с учетом категории и уязвимости объекта;

• разработка и адаптация новейших технологий и программно-аппаратных средств обеспечения безопасности, в том числе пассивных и активных средств защиты критически важных и опасных объектов инфраструктуры железнодорожного транспорта;

• создание автоматизированной системы мониторинга состояния и управления безопасностью критически важных и опасных объектов инфраструктуры;

• подготовка специалистов в области обеспечения транспортной безопасности;

• осуществление автоматизированного контроля и надзора в области обеспечения транспортной безопасности;

• создание, модернизация и ведение баз данных по оценке уязвимости категорированных объектов;

• разработка и ведение планов обеспечения транспортной безопасности категорированных объектов;

• паспортизация категорированных объектов;

• мониторинг состояния транспортной безопасности на железнодорожном транспорте, включая создание и эксплуатацию центра контроля состояния транспортной безопасности;

• оснащение (модернизация) объектов железнодорожного транспорта техническими средствами защиты.

Для решения указанных задач требуется разработка комплекса нормативных, организационных, экономических и технико-технологических мероприятий.

Также потребуется совершенствование деятельности всех органов управления транспортом, модернизация производственной

базы транспорта, переход на новые технологии и виды технических средств, активное использование новейших информационно-коммуникационных технологий и средств их реализации (средств вычислительной техники и связи, сбора и обработки информации).

Комплексным результатом реализации таких мероприятий будет создание эффективной системы обеспечения необходимого уровня защищенности объектов инфраструктуры железнодорожного транспорта для устойчивого и безопасного функционирования транспортной системы и защиты ее от актов незаконного вмешательства.

На сегодняшний день деятельность по управлению защитой информации компании направлена на обеспечение безопасности информации объектов инфраструктуры, а также на сохранение конфиденциальности, целостности и доступности информации и единства информационного пространства ОАО «РЖД».

К основным объектам защиты информации, согласно открытым источникам в ОАО «РЖД», относятся:

- объекты информационной инфраструктуры, включающие в себя программно-технические комплексы и систему управления единой магистральной цифровой сетью связи (ЕМЦСС);
- системы управления автоматических телефонных станций общетехнологической и оперативно-технологической сетей;
- программно-технические комплексы и система управления сетью передачи данных (СПД);
- объекты автоматизированных систем управления и информационных систем, включающие в себя отдельные автоматизированные рабочие места (АРМ) и локальные вычислительные сети (ЛВС), серверные сегменты информационных систем и автоматизированных систем управления, программно-технические комплексы поддержания специализированных баз данных;
- системы документооборота.

Существует три основных составляющих защиты: организационная, нормативно-правовая и техническая. Организационная составляющая включает в себя должностных лиц и штатные подразделения обеспечения информационной безопасности. Нормативно-правовая составляющая разрабатывается на основе действующих

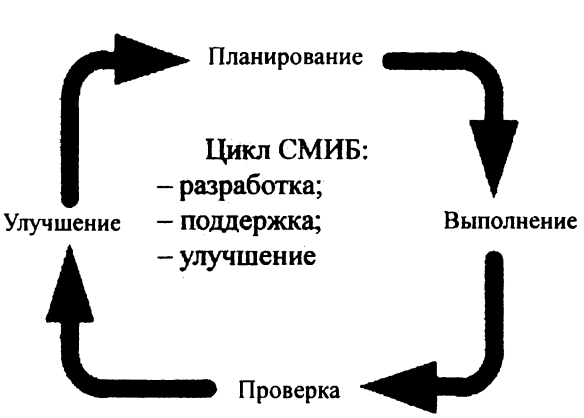
в Российской Федерации законодательных и нормативных документов и международных стандартов: ГОСТ Р 51275-99; ГОСТ Р 51624-2000; ГОСТ Р 51583-2000; ГОСТ Р ИСО/МЭК 15408-2002; ISO/IEC 17799:2005; ISO/IEC 27001:2005 и др. Также ОАО «РЖД» использует ряд корпоративных стандартов управления защитой информации, политик информационной безопасности, положений, регламентов и т. д. В качестве примеров нормативных актов можно привести «Инструкцию о порядке обращения с информацией, составляющей коммерческую тайну ОАО "РЖД"», распоряжение «Об организации работ по предотвращению записи, хранения и распространения информации и программных продуктов непроизводственного характера» с «Примерным перечнем категорий информации и программных продуктов...» и «Примерным порядком организации создания корпоративных Web-сайтов, FTP-серверов, конференций...», «Порядок подключения пользователей к информационным ресурсам ОАО "РЖД"» и др.

Техническую составляющую представляет корпоративная инфосеть, которая объединяет информационные ресурсы и технические средства обработки и передачи информации центрального аппарата, железных дорог и других филиалов РЖД.

Таким образом, проведя предварительный аудит и оценив активы организации и их важность, можно определить приоритетные направления разработки в системе менеджмента информационной безопасности (СМИБ) [2]. Исходная концептуальная модель СМИБ приведена на рисунке.

Следующий перечень процессов призван модернизировать, укрепить и улучшить действующие регламенты по безопасности, а также развить инновационный подход [3]:

- Распределение обязанностей и ответственности.
- Повышение осведомленности сотрудников в вопросах информационной безопасности.
- Обеспечение непрерывности бизнес-процессов.
- Мониторинг информационной инфраструктуры.
- Безопасное хранение данных.
- Управление доступом к данным.




Модель СМИБ

- Управление информационной инфраструктурой.
- Управление изменениями.
- Управление инцидентами и уязвимостями.
- Защита от вредоносного кода.
- Взаимодействие с третьими сторонами.
- Безопасная разработка программного обеспечения.
- Управление аутентификацией и парольная защита.
- Обеспечение физической безопасности.
- Криптографическая защита и управление ключами.

Часть процессов уже находится в исполнении. Другую часть необходимо регламентировать и утвердить в стандартах по защите информации. Ответственность за действия по обеспечению информационной безопасности возлагается на департамент безопасности ОАО «РЖД».

Наиболее важный принцип – это функциональная интеграция специализированных программно-технических комплексов защиты с программно-техническими комплексами передачи и обработки информации, имеющими собственные встроенные средства защиты с мощной функциональностью (например, ОС рабочих станций и серверов, активное сетевое оборудование). Функциональная интеграция позволяет достигать высокого уровня защищенности при минимизации затрат на внедрение.

Также важно практикуемое сегментирование сети по территориально-производственной принадлежности с разделением функций и ролей. Это означает физическое или виртуальное разделение локальных вычислительных сетей и информационных ресурсов структурных единиц ОАО «РЖД» с жестким распределением прав доступа к ресурсам между персоналом.

Важным пунктом является инфраструктура Windows-доменов и ActiveDirectory (AD), которая дает возможность централизованного формирования и управления политиками безопасности информационных систем.

Также можно упомянуть и инфраструктуру открытых ключей, предназначенную для усиленной аутентификации и авторизации доступа к информационным ресурсам функционирования VPN-каналов, а также реализации шифрования и электронной цифровой подписи при внутреннем информационном обмене.

К общим техническим компонентам отнесем комплекс защиты от разрушающих программных воздействий и обновлений ПО, поддерживающий оперативную рассылку обновлений антивирусных баз и системного программного обеспечения по всей сети филиалов компании.

Помимо всего прочего, особо важными являются действия сотрудников ОАО «РЖД» при работе с объектами защиты. Необходимо, чтобы каждый сотрудник следовал установленным регламентам. При работе с данными сотрудник должен:

1) организовывать работу по выполнению нормативных документов и рекомендаций ОАО «РЖД» в части обеспечения информационной безопасности;

2) обеспечивать функционирование системы защиты информации при взаимодействии с информационными ресурсами ОАО «РЖД» и сетью передачи данных ОАО «РЖД»;

3) принимать необходимые меры при обнаружении попыток несанкционированного доступа к информационным ресурсам ОАО «РЖД»;

4) предоставлять работникам право доступа на объекты информатизации по служебному удостоверению;

5) незамедлительно информировать департамент безопасности ОАО «РЖД» о фактах утечки информации, составляющей коммерческую тайну ОАО «РЖД»;

6) устанавливать программные продукты, необходимые для пользования системами обеспечения информационной безопасности ОАО «РЖД», на оборудование, имеющее доступ к сети передачи данных ОАО «РЖД»;

7) участвовать в служебных расследованиях, проводимых департаментом по безопасности по фактам, обнаруженным в ходе проверок обеспечения информационной безопасности;

8) выполнять мероприятия по устранению уязвимостей и нарушений в обеспечении защиты информации информационных систем и сетей в соответствии с уведомлениями департамента безопасности.

Таким образом, в сумме все мероприятия должны дать положительный эффект, а также сопутствовать укреплению, модернизации, общему улучшению и инновационным изменениям в сфере защиты информации в структуре ОАО «РЖД».

## Библиографические ссылки

1. О стратегии развития железнодорожного транспорта в Российской Федерации : портал ОАО «РЖД». URL: http://doc.rzd.ru/doc/public/ru?STRUCTURE_ID=704&layer_id=5104&id=3997 (дата обращения: 20.10.2013).

2. *Доценко С. П.* Подход к построению модели систем менеджмента информационной безопасности // Науч. журн. КубГАУ. 2009. Вып. № 53(9). С. 6–9.

3. Стандарты ISO 27000 [Электронный ресурс]. URL: www.iso27000.ru/standarty (дата обращения: 20.10.2013).